

بوعافية رشيد — **المركز الجامعي خميس مليانة**

ابراهيم مزيود — **جامعة الدكتور فارس يحي بالمدية**

مداخلة بعنوان:

التحول إلى وسائل الدفع الالكترونية وتحديات الجرائم المعلوماتية

مقدمة

افرز التطور الهائل لتكنولوجيا المعلومات والاتصال عدة تغييرات ومستجدات على كل القطاعات بما فيها القطاع المالي والمصرفي الذي ظهر به منتجات وخدمات مالية جديدة اتجه التعامل بها على نطاق واسع ومن أي مكان بفعل الترابط الأسواق المالية والتي عززتها تكنولوجيا الاتصال ،بالرغم من المزايا التي وفرتها أساليب الدفع الحديثة إلا أنها أفرزت تحديات جديدة والمتمثلة في جرائم المعلوماتية كنمط جديد من جرائم الاقتصادية والمالية التي أصبحت تهدد القطاع المالي ووسائل دفعه الحديثة خاصة في ظل الخصائص التي تتميز بها هذا النوع من الجرائم والآليات الضرورية لمكافحتها خاصة من الجانب القانوني وهذا ما سيتم اظهاره في هذه الورقة البحثية من خلال المحاور التالية:

أولا : وسائل الدفع الالكترونية.

ثانيا : الجريمة المعلوماتية

ثالثا : صور الجرائم المعلوماتية على وسائل الدفع الحديثة.

رابعا: التجارب الدولية العربية في مكافحة جرائم المعلوماتية

أولا : وسائل الدفع الالكترونية.

1.**مفهوم وسائل الدفع الالكترونية**

وسائل الدفع المتطورة في الانترنت هي عبارة عن الصورة أو الوسيلة الالكترونية التقليدية للدفع و التي نستعملها في حياتنا اليومية، الفرق الأساسي بين الوسيلتين هي أن وسائل الدفع الالكترونية تتم كل عملياتها و تسير الكترونيا، و لا وجود للحوالات و لا للقطع النقدية [1]

ويتميز الدفع الإلكتروني بالخصائص التالية :

-**يتسم الدفع الالكتروني بالطبيعة الدولية،** أي أنه وسيلة مقبولة من جميع الدول، حيث يتم استخدامه لتسوية الحساب في المعاملات التي تتم عبر فضاء الكتروني بين المستخدمين في كل أنحاء العالم خاصة بما أن عمليات التجارة تتوسع إقليميا و دوليا، و بذلك تساعد وسائل الدفع الالكترونية على تحسين السيطرة على عمليات التوزيع و النقل[2] .

-**يتم الدفع باستخدام النقود الالكترونية،** وهي قيمة نقدية تتضمنها بطاقة بها ذاكرة رقمية أو الذاكرة الرئيسية للمؤسسة التي تهيمن على إدارة عملية التبادل،

-**يستخدم هذا الأسلوب لتسوية المعاملات الالكترونية عن بعد،** حيث يتم إبرام العقد بين أطراف متباعدة في المكان، و يتم الدفع عبر شبكة الانترنت، أي من خلال المسافات بتبادل المعلومات الالكترونية بفضل وسائل الاتصال اللاسلكية، يتم إعطاء أمر الدفع وفقا لمعطيات الكترونية تسمح بالاتصال المباشر بين طرفي العقد،

2.**أنواع وسائل الدفع الالكترونية**

تتمثل أهم أنواع وسائل الدفع الالكترونية فيما يلي:

- **البطاقات البنكية :**

تعرف البطاقة البنكية على أنها كل بطاقة تسمح لحاملها بسحب أو بنقل الأموال، و لا يمكن أن تصدر إلا من طرف هيئة قرض أو مؤسسة مالية أو مصلحة مرخص لها بوضع و إصدار البطاقات كالمصارف، الخزينة العامة، مصالح البريد[3].

فالبطاقات البنكية هي عبارة عن بطاقة بلاستيكية و مغناطيسية يصدرها البنك لصالح عملائه بدلا من حمل النقود"، فهي بطاقة بلاستيكية مستطيلة الشكل تحمل اسم المؤسسة المصدرة لها، و شعارها و توقيع حاملها، و بشكل بارز على وجه الخصوص رقمها، و اسم حاملها و رقم حسابه و تاريخ انتهاء صلاحيته[4]".

البطاقات الذكية: ظهرت البطاقة الذكية على اثر المشاكل التي عرفتها البطاقات السابقة كبقات الائتمان والتي اخترعت سنة **1975** وبدا استعمالها من طرف شركة فليبس والباقة الذكية عبارة عن و هي عبارة عن بطاقة بلاستيكية ذات حجم قياسي تحتوي في داخلها على شرائح للذاكرة تعمل بواسطة ميكروكومبيوتر يزودها بطاقة تخزينية للبيانات أكبر بكثير من تلك التي تستوعبها البطاقات ذات الشرائط الممغنطة و لكنها أعلى منها تكلفة، و تقدم هذه البطاقة العديد من الخدمات، منها بعض

البيانات الشخصية الخاصة بحاملها مثل التاريخ الطبي للشخص و معلومات عن حساباته الشخصية المصرفية.

- **النقود الالكترونية :** عرف النقود الالكترونية حسب صندوق النقد الدولي على أنها قيمة نقدية في شكل وحدات ائتمانية مخزنة في شكل الكتروني أو في ذاكرة الكترونية لصالح المستهلك[5] ، وبهذا فان النقود الالكترونية عبارة عن المكافىء للنقود التقليدية إلا أن وحدة النقد فيها في وحدة النقد الرقمي أو الالكتروني وتأخذ النقود الالكترونية صورتين[6] :

 الصورة الأولى هي البطاقات السابقة الدفع المعدة للاستخدام في أغراض متعددة و يطلق عليها أيضا تعبير البطاقات مختزنة القيمة أو محفظة النقود الالكترونية.

الصورة الثانية: هي آليات الدفع مختزنة القيمة أو سابقة الدفع التي تمكن من إجراء مدفوعات من خلال استخدام شبكات الحساب الآلي المفتوحة خاصة الانترنت ؛ و التي يطلق عليها أحيانا نقود الشبكة أو نقود السائلة الرقمية

الشيك الإكتروني.

- **المحافظ الالكترونية:**

المحافظ الالكترونية تقوم بتحويل النقد إلى سلسلة رقمية، و تخزن على القرص الثابت في موقع العمل، و هذا يحد من استخدام النقود في المعاملات التي تتم على شبكة الانترنت، و معظم الحقائب الالكترونية تقوم بتخزين النقد الالكتروني على البطاقات الذكية التي تتمكن من دفع أي مبلغ من الحقيبة الالكترونية في أي مكان[7].

- **الشيكات الالكترونية:**

الشيك الالكتروني عبارة عن بيانات يرسلها المشتري إلى البائع عن طريق البريد الالكتروني المؤمن، و تتضمن هذه البيانات التي يحتويها الشيك البنكي من تحديد مبلغ الشيك و اسم المستفيد و اسم من أصدر الشيك و توقيعه، و يكون هذا التوقيع عن طريق رموز خاصة (1).

فيمكن تعريفه بأنه "رسالة موثقة و مؤمنة يرسلها مصدر الشيك إلى مستلم الشيك (حامله) ليعتمده و يقدمه للبنك الذي يعمل عبر الانترنت ليقوم البنك أولا بتحويل قيمة الشيك المالية إلى حساب حامل الشيك و بعد ذلك يقوم بإلغاء الشيك و إعادته الكترونيا إلى مستلم الشيك (حامله) ليكون دليلا على أنه قد تم صرف الشيك فعلا و يمكن لمستلم الشيك أن يتأكد من أنه قد تم بالفعل تحويل المبلغ لحسابه". [9]

ثانيا : الجريمة المعلوماتية

1.تعريف الجريمة المعلوماتية

تعرف الجريمة عموما في نطاق القانون الجنائي بأنه سلوك الفرد عملا كان أو امتناعا يواجهه المجتمع بتطبيق عقوبة جنائية، أما المعلوماتية فهي مشتق من المعلومات

أما الجريمة المعلوماتية فقد تعددت التعاريف وتباينت ومن جملة هذه التعاريف نجد :

كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية [10].

وتعرف أيضا على أنها فعل أو امتناع عمدي ينشأ عن نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة في الحاسب ، أو التي تحوَل عن طريقه[11].

وقد عرفت منظمة التعاون الاقتصادي والتنمية **OCDE** لجريمة المعلوماتية على أنها : كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[12].

ويعد هذا التعريف أوضح تعريف أكثر شمولا مما سبق وهذا لمراعاة الاعتبارات التالية :

- تلاؤم هذا التعريف مع فكرة عالمية المعلومات والاتصالات، إذ انه تعريف مقبول ومفهوم على المستوى العالمي.
- مراعاة التعريف للتطور المتلاحق لتكنولوجيا الحسابات الآلية بصفة خاصة ،بحث لا يقتصر على التكنولوجيا الراهنة ،بل يسمح باستيعاب ما قد يجد من صور للجريمة المعلوماتية نتيجة تطور المعلومات.
- وأخيرا لما كانت الجريمة المعلوماتية يمكن أن تنطوي على أشكال مختلفة للسلوك الإجرامي ابتداء من القيل إلى الاعتداء على حرمة الحياة الخاصة فيجب أن يوضح التعريف خصوصية الجريمة المعلوماتية بحيث يبدو واضحا الدور الذي يقوم به الحساب الآلي والمعلومات في ارتكاب الجريمة.

2.خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بطيعة خاصة تميزها عن غيرها من الجرائم التقليدية وذلك نتيجة لارتباطها بتقنية المعلومات والحاسب الآلي مع ما يتمتع به من تقنية عالية وقد كان لظهور شبكة الانترنت في إضفاء شكل جديد للجريمة المعلوماتية هو الطبيعة الدولية أو متعددة الحدود.

- **خصائص تشترك فيها مع بعض الجرائم:**

 خطورة الجرائم المعلوماتية : وذلك لمساسها بالإنسان في فكره وحياته ،وتمس المؤسسات في اقتصادها والبلاد في أمنها القومي والسياسي والاقتصادي ،ومن شأن ذلك أن يضفي إبعادا خطيرة غير مسبوقة على حجم الإضرار والخسائر التي تنجم عن ارتكاب هذه الجرائم على مختلف القطاعات والمعاملات ولا أدل على ذلك من أن حجم الخسائر المادية الناجمة عن هذه الجرائم قد لغت وفقا لما بينته الإحصاءات في فرنسا طبقا للجمعية العمومية ضد الحرائق والمخاطر سنة **1986** قدرت بـ **7.3** مليار فرنك فرنسي،

 الطبيعة المتعدية الحدود:

من أهم خصائص التي تميز الجريمة المعلوماتية هي تخطيها للحدود الجغرافية ومن اكتسابها طبيعة متعددة الحدود ، فبعد ظهور شبكات المعلومات لم تعد الحدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة ،فالقدرة التي تتمتع بها الحسابات الآلية في نقل وتبادلا كميات كبيرة من المعلومات بين أنظمة يفصل بينها ألاف الأميال ،قد أدت إلى نتيجة

مؤداها إن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة المعلوماتية وحجم المعلومات والأموال المستهدفة والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال

وقد أثارت الطبيعة الدولية للجرائم المعلوماتية تساؤلا مهما يتعلق بتحديد الدولة التي يختص قضاؤها بملاحقة الجريمة ،ام تلك التي أضرت مصالحها نتيجة لهذا التلاعب ،كما أثرت هذه الطبيعة أيضا الشكوك حول مدى فاعلية القوانين القائمة في التعامل مع الجريمة المعلوماتية وبصفة خاص فيما يتعلق بجمع وقبول الأدلة.

خصائص تتفرد بها الجريمة المعلوماتية عن الجرائم الأخرى

تختلف الجريمة المعلوماتية عن باقي أنواع الجرائم في :

- **تتطلب لارتكابها وجود كمبيوتر ومعرفة تقنية باستخدامها :**

تختلف الجريمة المعلوماتية عن باقي أنواع الجرائم في :

- **تتطلب لارتكابها وجود كمبيوتر ومعرفة تقنية باستخدامها :**

حيث يعتبر الاستعانة بجهاز الكمبيوتر أساسا لارتكاب الجريمة المعلوماتية وليس سرقة الجهاز أو إتلافه لأنه يدخل في تطاق الاعتداء أو سرقة الأموال المادية المنقولة، وترتكب الجريمة بتدمير برامج الكمبيوتر أو سرقتها أو العبث بالبيانات أو المعلومات المخزنة [13].

كما تعتمد هذه الجرائم على قمة الذكاء في ارتكابها ويصعب على المحقق التقليدي التعامل مع هذه الجرائم ،إذ يصعب عليه متابعة الجرائم المعلوماتية والكشف عنها وإقامة الدليل عليها، فهي جرائم تتسم بالغموض وإثباتها بالصعوبة بمكان والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية،كما انه كلما تقدمت المعرفة التقنية كلما زادت احتمالية توظيف هذه المعارف بشكل غير مشروع وزيادة خطورة الجرائم المعلوماتية.

- **صعوبة اكتشافها وإثباتها:**

تتسم الجريمة المعلوماتية بأنها لا تترك اثر بعد ارتكابها علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت[14] ، فليس هناك أموال مادية منقولة تم اختلاسها وإنما هي أرقام تتغير في السجلات، كما أن معظم الجرائم المعلوماتية تم اكتشافها بالمصادفة وبعد مرور وقت طويل إضافة انه لا يتم في الغالب الإبلاغ عن الجرائم المعلوماتية أما لعدك اكتشافها من طرف الضحية أو خوفا من التشهير به لذلك ما يرتكب فعلا من جرائم معلوماتية اكبر بكثير ما يصرح به.

- **تميز مرتكب الجريمة المعلوماتية عن غيره من مرتكبي الجرائم الأخرى :**

يتصف مرتكبوا الجرائم المعلوماتية بعد صفات تميزهم عن غيرهم من المتورطين في أشكال الإجرام الأخرى والمتمثلة ف

حيث يعتبر الاستعانة بجهاز الكمبيوتر أساسا لارتكاب الجريمة المعلوماتية وليس سرقة الجهاز أو إتلافه لأنه يدخل في تطاق الاعتداء أو سرقة الأموال المادية المنقولة، وترتكب الجريمة بتدمير برامج الكمبيوتر أو سرقتها أو العبث بالبيانات أو المعلومات المخزنة[15].

كما تعتمد هذه الجرائم على قمة الذكاء في ارتكابها ويصعب على المحقق التقليدي التعامل مع هذه الجرائم ،إذ يصعب عليه متابعة الجرائم المعلوماتية والكشف عنها وإقامة الدليل عليها، فهي جرائم تتسم بالغموض وإثباتها بالصعوبة بمكان والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية،كما انه كلما تقدمت المعرفة التقنية كلما زادت احتمالية توظيف هذه المعارف بشكل غير مشروع وزيادة خطورة الجرائم المعلوماتية.

- **صعوبة اكتشافها وإثباتها:**

تتسم الجريمة المعلوماتية بأنها لا تترك اثر بعد ارتكابها علاوة على صعوبة الاحتفاظ الفني بآثارها إن وجدت[16] ، فليس هناك أموال مادية منقولة تم اختلاسها وإنما هي أرقام تتغير في السجلات، كما أن معظم الجرائم المعلوماتية تم اكتشافها بالمصادفة وبعد مرور وقت طويل إضافة انه لا يتم في الغالب الإبلاغ عن الجرائم المعلوماتية أما لعدك اكتشافها من طرف الضحية أو خوفا من التشهير به لذلك ما يرتكب فعلا من جرائم معلوماتية اكبر بكثير ما يصرح به.

- **تميز مرتكب الجريمة المعلوماتية عن غيره من مرتكبي الجرائم الأخرى :**

يتصف مرتكبوا الجرائم المعلوماتية بعد صفات تميزهم عن غيرهم من المتورطين في أشكال الإجرام الأخرى والمتمثلة في :

ثانيا : صور الجرائم المعلوماتية على وسائل الدفع الحديثة.

تتمثل الظواهر الأكثر بروزا لجرائم المساس بأنظمة الكومبيوتر و الانترنت في:

أولا : جريمة النصب بالتجارة الالكترونية

تواجه كثير من الشركات الممارسة للتجارة الإلكترونية مشكلات أمنية مهمة، مثل تعرض البيانات والتدخل أو التشويش على المواقع، حيث لازال هناك الكثير من محترفي الحاسوب يحاولون اختراق المواقع الإلكترونية، كما تخشى الشركات أيضا من أولئك الذين لديهم مهارات اختراق أنظمة الحاسوب بغرض التجسس على معلومات تلك الشركات أو استبدال البيانات ومن ثم الإستخدام الزائف لها.

وهذا باستخدام شبكة الانترنت التي تعد قوام التجارة الالكترونية بأساليب متعددة وذلك في الحالات التي قد يستخدم فيها حامل البطاقة بطاقته في شراء بعض السلع والمنتجات عبر الشبكة حيث يستطيع قراصنة الانترنت الحصول على بيانات البطاقة بأساليب احتيالية ويستخدمونها في الحصول على مزيد من هذه السلع والمنتجات ،التي يفاجأ صاحب البطاقة بمطالبته بثمنها رغم عدم شرائه لها[17][1].

: جريمة غسل الأموال عبر الوسائل الالكترونية

لقد تعددت تعاريف ظاهرة غسيل الأموال فلا يوجد تعريف موحد اتفق عليه بسبب تعدد مصادر الأموال غير المشروعة،وتنوع طرق ووسائل الغسيل وتباين وجهات النظر حول المصادر التي يجب أن تكون هدف التجريم في إطار مكافحة غسيل الأموال،ومن بين التعاريف التي جاءت لتحديد الظاهرة ما يلي :

---

[1] محمد علي قطب ، الجرائم المعلوماتية وطرق مواجهتها، مرجع سبق ذكره ص 08

غسيل الأموال هو تلك العمليات التي تشمل مجموع الأنشطة التي تتم بعيداُ عن أجهزة الدولة ولا تسجل في حسابات الدخل القومي، وهذه الأنشطة تمثل مصدر للأموال القذرة التي يحاول أصحابها غسيلها في مرحلة تالية، وذلك بإجراء مجموعة من العمليات والتحويلات المالية والعينية على الأموال القذرة لتغيير صفتها غير المشروعة في النظام الشرعي وإكسابها صفة مشروعة[18].

وفي تعريف أكثر تحديد فان غسيل الأموال هو

وتتمثل مصادر غسيل الأموال في[19]:

- المخدرات و المؤثرات العقلية، و التجارة غير المشروعة في الأسلحة النارية و الذخائر.
- جرائم الإحتيال و خيانة الأمانة و ما يرتبط بهما من تجسس و تزوير النقود.
- جرائم الإختلاس و الرشوة و الإضرار بالأموال العامة.
- تجارة الجنس، الدعارة و ما يرتبط بهما.
- الجرائم المختلفة لمخالفة أحكام قانون البيئة.

ومع تطور القطاع المالي والمصرفي كغيره من القطاعات مع تطور التكنولوجية المصاحبة للعولمة تطورت معه أساليب تقديم الخدمات المالية والمصرفية وبالمقابل فان عصابات الجريمة المنظمة وغاسلي الأموال استفادوا من هذه التكنولوجية وبالتحديد من المخاطر المصاحبة لاستخدامها وبذلك فقد تطورت وتغيرت وسائل وطرق غسيل الأموال وأصبحت تبتعد تدريجيا عن الأساليب التقليدية التي تكون عرضة للاشتباه فيها وكشفها بسهولة ، وفيما يلي توضيحا لأهم هذه الأدوات والأساليب الالكترونية[20].

- **أجهزة ATM :**

يتم استخدام هذه الآلات في غسيل الأموال من خلال إجراء العديد من عمليات الإيداع والسحب للأموال لضمان عدم الكشف ولفت الانتباه،وتحاشيها للالتزامات القانونية المترتبة على البنوك بالإبلاغ عن عمليات الإيداع والسحب التي تتجاوز المبالغ المحددة رقابيا.

- **بنوك الانترنت :**

ان شبكة الانترنت أدت إلى نشوء التجارة الالكترونية والتي يمكن ان يتم عن طريقها إجراء العديد من الصفقات المشبوهة وغير القانونية والتي تسهم في عمليات غسيل الأموال ،مستغلين في هذا الصعوبة التعرف على البطاقة الشخصية وعناوين إقامة المتعاملين مع المصارف الدولية التي تتعامل عبر شبكة الانترنت.

- **الخدمات المصرفية الالكترونية:**

تستخدم الخدمات المصرفية الالكترونية في عمليات غسيل الأموال وخاصة في مرحلتي التوظيف والدمج كالتحويل الالكتروني للأموال ودفع الفواتير .... وغيرها.

- **الاتصالات الالكترونية:**

تعد الاتصالات الالكترونية من أشكال الاتصالات غير الخاضعة للقيود والضوابط الرقابية والتي من أهمها البريد الالكتروني وغرف المحادثة ... وغيرها، حيث يستطيع غاسلي الأموال استغلال هذه الوسائل في اتصالاتهم وخططهم لتنفيذ عملياتهم الإجرامية نوفي القيام بطرح معلومات مضللة وغير دقيقة حوا أسعار

الأسهم بهدف تضليل المستثمرين فيستغلها غاسلي الأموال في تحقيق الأرباح الطائلة من عمليات البيع والشراء واليت من شأنها أن توفر الغطاء القانوني واللازم للأموال القذرة التي يغسلوها.

- **النقود الالكترونية:**

وهي من أهم الأدوات الالكترونية لغاسلي الأموال وذلك لاستحالة تعقبها وسريتها سرعتها حيث يمكن تحويل أي مبلغ من خلالها في فترة قصيرة من دون إعاقات جغرافية أو قانونية أو مصرفية وبدون حاجة للوسيط المالي.

ثالثا : جرائم أخرى مرتبطة بالكمبيوتر

إضافة إلى جرائم الأموال عبر التجارة الالكترونية وجرائم غسيل الأموال هناك جرائم أخرى ترتبط باستعمال جهاز الكمبيوتر والمتمثلة في :

1. **جرائم الفيروسات :**

برنامج خبيث يتم إدخاله في نظام بدون علم المستعمل. و لدى هذا البرنامج القدرة على استنساخ نفسه (سواء في شكل مطابق تماماً أو، في حالة الفيروس متعددة الأشكال، بالطفرات)، وذلك للإضرار بالبيئة التي يتم تنفيذ ذلك فيها، ولتلويث المستعملين الآخرين الذين يتلامسون معه. وهناك أنواع مختلفة من الفيروسات، تبعاً لتوقيعاتها، وسلوكها وكيفية تكاثرها، وكيفية نقل العدوى للماكينات، والأعطال التي تسببها، الخ. فالديدان، أحصنة طروادة والقنابل المنطقية هي شفرات خبيثة تنتمي إلى عائلة الفيروسات التنوعية[21] .

وتعد الفيروسات اخطر العناصر التي تهدد امن البرامج والبيانات لأنها تؤدي إلى فقد النظام أو فقد تكامله أو تؤثر على كفاءة أدائه كما تؤدي إلى إتلاف البرامج وضياع المعلومات .

وتنتقل الفيروسات أما من خلال استخدام برنامج غير أصلي أومن خلال البريد الالكتروني وشبكات الاتصال.

وتتمثل إعراض الإصابة بالفيروس فيما يلي:

- بطء تشغيل الجهاز
- توقف النظام عن العمل
- نقص شديد في سعة الذاكرة
- ظهور حروف غريبة عند الضغط علة مفاتيح معينة
- تغيير في حجم الملفات وعددها
- عرض رسالة خطأ فجائية وغير عادية
- تشغيل القرص أكثر من المعتاد.

---

[2] 2007 118

رابعا : التجارب الدولية العربية في مكافحة جرائم المعلوماتية :

1.مكافحة جرائم المعلوماتية في الولايات المتحدة الأمريكية.

إن الولايات المتحدة الأمريكية ، لا تتميز بأسبقية سن هذه التشريعات فحسب بل تتميز بسن تشريعات خاصة بكافة مسائل تقنية المعلومات وفي قطاعات الحوسبة والاتصالات والانترنت ترتبط او تتعلق بجرائم الكمبيوتر والانترنت مباشرة او على نحو غير مباشر ، كما أنها تشريعات تراعي خصائصها المميزة وتتطور تبعا لتطور قطاع التقنية ذاته ، وتتميز الولايات المتحدة الأمريكية أيضا بوضع عدة تشريعات على المستوى الفدرالي وحزمه معتبرة من التشريعات على مستوى الولايات. فعلى المستوى الفدرالي، تبلور نشاط لجنة الكونجرس الخاصة بحماية استخدام الحاسوب بتقديم مشروع (قانون حماية الحاسوب سنة 1984) غير أن هذا المشروع لدى عرضه ودراسته من قبل الكونجرس ولجانه المختصة ، جرى التعديل على أحكامه بشكل جوهري ، وجرى إقراره بعد سلسلة من التعديلات والإضافات ولم يصدر باسمه المشار إليه ، فصدر قانون (غش الحاسوب وإساءة استخدامه لعام 1984) أو كما يترجم اسمه البعض (قانون الاحتيال وإساءة استخدام الحاسوب - Computer Fraud and abuse Act .) وأضيف إلى القانون مدونة القانون الأمريكي تحت قسم الجرائم .

وقد نص القانون المذكور، على تجريم مجرد الاتصال دون تصريح بنظام حاسوب ، وعلى الاتصال المصرح به الذي يستخدم فيه الفاعل الحاسوب لأغراض غير مصرح بها كتعديل أو إتلاف أو تدمير أو افشاء المعلومات المخزنة في الحاسب، كما نص على عقاب من يرتكب فعلا من شأنه منع الاستخدام المصرح به للحاسوب" ، وخضع لاحقا لتعديلات واكبت التطورات التقنية . كما صدر ايضا في الولايات المتحدة على المستوى الفدرالي (قانون أمن الحاسوب لسنة 1987) والذي يقضي باتخاذ الوكالات الفدرالية خطوات ملائمة لتأمين وحماية أنظمة حواسيبها، وينظم هذا القانون مستويات الحماية والرقابة عليها والمسؤولية عن اغفالها. وتوالت بعد ذلك في التسعينات التعديلات والتشريعات الفرعية والقطاعية ذات العلاقة بامن المعلومات.

أما على مستوى الولايات ، فقد سنت جميع الولايات – عدا واحدة - ، قوانين خاصة أو عدلت قوانين العقوبات لديها بما يكفل النص على تجريم أنشطة جرائم الحاسوب مع تباين فيما بينها سواء من حيث صور النشاط المجرم، أو من حيث آلية التعامل مع محل الاعتداء. فقد نصت قوانين بعض الولايات. على المساواة بين معطيات الحاسوب والأموال المادية من حيث الحكم القانوني مما يتيح انطباق نصوص التجريم التقليدية على جرائم الحاسوب باعتبارها تستهدف المعطيات المتخذة حكم الأموال المادية بنص القانون الصريح . من هذه الولايات مثلا ، ولاية ألاسكا ، التي أدخل قانونها الجديد الإتلاف المعلوماتي ضمن الأموال التي تخضع لنصوص الإضرار بالمال، وكذلك ساوى قانونها بين غش الانسان وغش الآلة ، وكذلك ولاية فرجينيا التي نص قانونها على اعتبار وقت أو خدمات الحاسوب، أو خدمات المعالجة الآلية للبيانات أو المعلومات أو البيانات المخزنة ذات الصلة بذلك مالا ، وبهذا الحكم يتحقق انطباق نصوص التجريم التقليدية فيما يتصل بالاعتداء على المال.

2.اتفاقية بودابست 2001 للجرائم الالكترونية[3].

بتاريخ **20** نيسان **2000** تقدمت اللجنة الأوروبية لمشكلات الجريمة **CDBC** ولجنة الخبراء في حقل جرائم التقنية – سايبر كرايم **CYBERCRIME** – (**pc-cy**) بمشروع اتفاقية جرائم الكمبيوتر وخضعت مواد الاتفاقية المقترحة للمناقشة وتبادل الآراء خلال الفترة من إصدار مشروعها الأول وحتى إعداد مسودتها النهائية التي أقرت لاحقا في بودابست **2001** وتعرف باتفاقية بودابست **2001** (اتفاقية الجرائم الالكترونية – سايبر كرايم) وكان قد طرح مشروع الاتفاقية للعامة ووزع على مختلف الجهات وأطلق ضمن مواقع عديدة أوروبية وأمريكية على شبكة الانترنت لجهة التباحث وإبداء الرأي . وتعكس الاتفاقية الجهد الواسع والمميز للاتحاد الأوروبي ومجلس أوروبا ولجان الخبراء فيهما المنصبة على مسائل جرائم الكمبيوتر وأغراضها منذ أكثر من عشرة اعوام .

تتكون الاتفاقية من مقدمة وأربعة فصول، فبعد أن استعرضت المقدمة أهداف الاتفاقية ومنطلقاتها ومرجعياتها السابقة وما تقوم عليه من جهود إرشادية وتوجيهية وتدابير إقليمية ودولية ، جاء الفصل الأول لتغطية المصطلحات الأساسية (مادة **1**) ، تضمن الفصل الثاني الذي جاء تحت عنوان الإجراءات المتعين اتخاذها على المستوى الوطني ، ثلاثة أقسام : الأول ، ويضم المواد من **2** – **13** ويعالج النصوص الموضوعية لجرائم الكمبيوتر ، والقسم الثاني ويضم المواد من **14** – **21** وتتعلق بالقواعد الإجرائية والقسم الثالث ويضم المادة **22** وتعلق بالاختصاص . اما الفصل الثالث من الاتفاقية والذي جاء تحت عنوان التعاون الدولي ، فقط تضمن قسمين ، الأول تحت عنوان المبادئ العامة ويضم المواد من **23**-**28** والقسم الثاني ويتعلق بالنصوص الخاصة ويضم المواد من **29**- **35** . أما الفصل الخامس فيتضمن الأحكام الختامية ويضم المواد من **36** – **48**

رابعا : واقع مكافحة الجرائم المعلوماتية في البيئة العربية.

إن عدم شيوع التكنولوجيا في البيئة العربية على نحو ما تشيع وتوظف في الدول المتقدمة ، يعكس أن البيئة العربية امن من الجرائم المعلوماتية لكن الحقيقة ليست كذلك ، اذ رغم انه لم تظهر وقائع وأحداث بحجم تلك التي تعيشها الدول المتقدمة ، لكن هذا لا يعني انه ليس هناك وجود لهذه الظاهرة عربيا ، عوضا عن ان مخاطر جرائم الكمبيوتر في بيئتنا قد تزيد عن مثيلاتها إذا ما قارنا مستويات الجاهزية التقنية والقانونية لمكافحة هذه الظاهرة ، وإذا كان مجرمو التقنية يركزون منذ أعوام على نظم الكمبيوتر والشبكات في الدول المتقدمة فان الوقت لن يطول قبل ان تتجه أنشطتهم لنظم المعلومات في الدول النامية او يولد في بيئاتنا من يساير أنشطتهم كما ظهر خلال الأعوام الخمسة الماضية.

وفي دراسة بحثية وتحليلية شاملة أجراها المركز العربي للقانون والتقنية العالية / عمان – الاردن (احد مؤسسات مجموعة عرب للقانون) في منتصف العام 2001 ، للوقوف على حجم هذه الظاهرة عربيا ، وجد

[3] [illegible] " [illegible] " [illegible] – [illegible] / [illegible] 4-2 [illegible] 2006 [illegible] 15-16-17 .

المركز ان نحو 23٪ من المؤسسات المشاركة في الدراسة (وعددها 1032 مؤسسة موزعة على 13 دولة عربية) قد عانت من صورة او اكثر من صور جرائم الكمبيوتر ، منها نحو 59٪ تعرضت لمشكلات خاصة بمواقعها على الانترنت تتراوح بين محاولات الاقتحام الى انكار الخدمة الى انشطة اساءة استعمال البريد الالكتروني اضافة الى انشطة اعتداء على امن التعاملات المالية على بعض هذه المواقع . وحول اساءة استخدام البريد الالكتروني اظهرت الدراسة ان اكثر من 82٪ من الانشطة غير المشروعة الموجهة للانظمة مصدرها مقاهي الانترنت العامة ، وان 73٪ من المؤسسات ليس لديها سياسة داخلية لتنظيم استخدام البريد الالكتروني من قبل موظفي المنشأة نفسها ، في حين ظهر ايضا وبنفس القدر تنامي الاهتمام بتنظيم قطاع المقاهي العامة للانترنت ، بحيث ارتفعت نسبة الوعي لمخاطر عدم التنظيم الى 86٪ عن الوضع السائد قبل عام 2001 . واحتلت هجمات الفايروس - التي ظهر ان مصدرها الخارجي بلغ 96٪ من نسبة الهجمات – المرتبة الاولى في الانشطة التي تعرضت لها المواقع العربية ونظم الكمبيوتر العربية ، ولم تتمكن الدراسة من تقديم ارقام موضوعية حول حجم الخسائر او معدلاتها ، وذلك للتباين الكبير بين الارقام التي قدمتها المؤسسات المشاركة وعلى نحو يظهر غياب اية معايير في البيئة العربية لحساب الخسائر الحقيقية الناجمة عن هذه الجرائم .

وفي البيئة العربية عموما ، ثمة نقص في الإحصاءات وتحليل عمليات الاختراق ، لكن هذا لا يعني عدم توفرها ، ومن اشهر حالات الاختراق – كما اشرنا اعلاه - الهجوم الذي تعرضت له شركة اتصالات الإمارات من قبل احد الهاكرز الذي يحمل جنسية بريطانية في العام الماضي ، كما تعرضت بعض المواقع المصرية الخاصة إلى أنشطة إنكار الخدمة وحصلت عدد من الحالات لدى بعض المواقع الأردنية ، حيث قام عدد من طلبة إحدى الجامعات الأردنية بإرسال رسائل بريد الكتروني بأسماء الغير متضمنة إساءات لشخص المرسل او المرسل إليهم كما كشف مؤخرا عن قيام احد الشباب حديثي السن بالشراء عبر الإنترنت باستخدام أرقام البطاقات المالية لأشخاص أردنيين وجرى كشف الحادثة ومتابعتها من خلال الشركة مصدرة البطاقات

وبصفة عامة عاجزة عن مواجهة خطر جرائم الكمبيوتر، ونقصد هنا خطر الجرائم الواقعة على البيانات المالية او المتعلقة بالذمة المالية ، فاذا ما اضيف الى هذا الواقع عدم وجود نصوص تجرم افعال الاعتداء على البيانات الشخصية المخزنة في نظم المعلومات وبنوكها او نصوصا تحمي البيانات من خطر المعالجة الآلية وتكفل حماية الخصوصية – بوجه عام طبعا وفي جميع الدول العربية– فاننا نكون امام واقع قاتم لن تزيل قتامته غير جهود وتدابير تشريعية حثيثة لسد النقص الحاصل وايجاد قواعد تحيط بهذا النمط الخطر والمستجد من أنماط الإجرام .

مواجهة جرائم المعلوماتية في القانون الجزائري :

لم تعرف الجزائر قوانين قبل **2004** تطبق بشكل خاص على نظام المعلوماتية أو على تكنولوجيات الإعلام والاتصال، ما عدا شبكة الاتصالات السلكية واللاسلكية ووسائل الإعلام السمعية.

ومراعاة لما شهدته الجزائر ويشهده العالم في الفترة الأخيرة وخاصة مع بداية الألفية الثالثة من تطورا كبيرا في مجال تكنولوجيات الإعلام و الاتصال التي تقوم بشكل اكبر على الاختراعات الجديدة في مجال الإلكترونيك والمعلوماتية ،ولمسايرة هذا التطور التكنولوجي كان لابد للدول من إيجاد الإطار القانوني المناسب بوضع النصوص الملائمة المختلفة استعمالات الإعلام الآلي وفي نفس السياق وضع قوانين خاصة لمواجهة ما يسمى بالإجرام المعلوماتي أو الجرائم الالكترونية.

وقد تجسد ذلك في الجزائر بصدور القانون رقم **04- 15** المؤرخ في **10** نوفمبر **2004** المعدل والمتمم لقانون العقوبات الذي نص على حماية جزائرية للأنظمة المعلوماتية من خلال تجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات.

وفي سنة **2009** صدر قانون رقم **09- 04** المؤرخ في **5** غشت سنة **2009** يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

خلاصة

تعد الجرائم المعلوماتية الشكل الحديث للجرائم المالية والاقتصادية التي ظهرت وتعدد أساليبها مع تطور وتعدد وسائل الدفع الالكترونية التي انتجتها تطور تكنولوجيا الاتصال والمعلومات وتختلف هذه الجرائم عن الجرائم التقليدية في صعوبة تحديد دليلها المالي وإمكانية تعديها للحدود القطرية للبلد مما أظهرت تحدي التكيف معها ومحاربتها خاصة في اطار القانوني وهذا بالرغم التجارب الدول المتقدمة في التعامل مع هذه الظاهرة.

اما على المستوى العربي فلا زالت الدول العربية حديثة التجربة مع هذه الظاهرة ولم تكيف نظمها القانوني مع هذه الظاهرة الجديدة لا سيما الجزائر بالرغم إصدارها مؤخرا لقانون مكافحة جرائم الكمبيوتر

الهوامش :

[1] : بن رجدال جوهر، "الانترنت و التجارة الالكترونية"، رسالة ماجستير، قسم علوم تسيير، كلية العلوم الاقتصادية

و علوم التسيير، جامعة الجزائر، 2002، ص 83.

[2] : محمد حسين منصور، "المسؤولية الالكترونية"، دار الجامعة الجديدة للنشر، الإسكندرية، 2003، ص 120.

[2] Jeantin Michel et Le Cannu Paul, "Droit Commercial – Instruments De Paiement Et De Crédit -Entreprise Difficulté -", 5° Edition, Précis Dalloz, Paris, 1999, p 2

[4] الرومي محمد أمين, "التعاقد الالكتروني عبر الانترنت", الطبعة الأولى, دار المطبوعات الجامعية, الإسكندرية, 2004.

[4] Hashem Moustafa Shérif et Serhouchi Ahmed, "La Monnaie Electronique", Edition Eyrolles, Paris, 1999, p 46.

[7]احمد جمال الدين موسى، النقود الالكترونية و تأثيرها على المصارف المركزية في إدارة السياسة النقدية، الجديد في أعمال المصارف من الوجهتين القانونية و الاقتصادية، أعمال المؤتمر العلمي السنوي لكلية الحقوق، جامعة بيروت العربية، الجزء الأول، الجديد في التقنيات المصرفية، منشورات الحلبي الحقوقية، بيروت2002، ص 121.

[8]حجازي بيومي عبد الفتاح، "النظام القانوني لحماية الحكومة الالكترونية"، الجزء الأول، مرجع سابق، ص 296.

[9] الرومي محمد امين مرجع سبق ذكره ص 145

[10] عفيفي كامل عفيفي ، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون – دراسة مقارنة - منشورات الحلبي الحقوقية - بيروت- **2003** - ص **32**

[11]يونس عرب ، موسوعة القانون وتقنية المعلومات ، دليل أمن المعلومات والخصوصية ، جرائم الكمبيوتر والانترنت ، الجزء الأول ، منشورات إتحاد المصارف العربية ، الطبعة الأولى ، ص **213**

[12] نادلة عادل محمد فريد قورة ، جرائم الحاسب الالي الاقاصلدية دراسة نظرية وتطبيقية، منشورات الحاتي الحقوقية 2005،ص32

[13] سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني ، العدد السابع ،ص 282

[14] جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي،دار النهضة العربية، الطبعة الأولى، **1992** ، ص**17**

[15] سميرة معاشي، ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني ، العدد السابع ،ص 282
[16] جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي،دار النهضة العربية، الطبعة الأولى، **1992** ، ص**17**
[17] محمد علي قطب ، الجرائم المعلوماتية وطرق مواجهتها، مرجع سبق ذكره ص 08
[18] صلاح الدين حسن السيسي، غسيل الأموال الجريمة التي تهد استقرار الاقتصاد الدولي، دار الفكر العربي، مدينة نصر، القاهرة، 2003
[19] حمدي عبد العظيم، غسيل الأموال في مصر و العالم، دار إيتراك، القاهرة، 1997، ص:24.
[20] رافعة إبراهيم الحمداني ، اثر استخدام التكنولوجيا المصرفية في ظاهرة غسيل الأموال والجهود الدولية لكافحتها
[21] دليل الأمن السيبراني للدول النامية، الاتحاد الدولي للاتصالات ، طبعة **2007**، ص **118**
[22] يونس عرب، قراءة في الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان، ورشة عمل " تطوير التشريعات في مجال مكافحة الجرائم الالكترونية " هيئة تنظيم الاتصالات / مسقط – سلطنة عمان **2**- **4** ابريل **2006**، ص ص **15**- **16**- **17** .